Open Cyber-Architecture for Electrical Energy Markets

M. Yuksel*, K. Bekris*, C. Y. Evrenosoglu†, M. H. Gunes*,
S. Fadali†, M. Etezadi-Amoli†, and F. Harris*
*CSE Department, University of Nevada - Reno, Reno, NV 89557.
†EBME Department, University of Nevada - Reno, Reno, NV 89557.
{yuksem, bekris}@cse.unr.edu, cevrenosoglu@unr.edu, mgunes@cse.unr.edu,
{fadali,etezadi}@unr.edu, fredh@cse.unr.edu

***Abstract*—Automated control and management of large-scale physical systems is a challenging problem in a wide variety of applications including: power grids, transportation networks, and telecommunication networks. Such systems require (i) data collection, (ii) secure data transfer to processing centers, (iii) data processing, and (iv) timely decision making and control actions. These tasks are complicated by the vast amount of data, the distributed sources of data, and the need for efficient data communication. In addition, large physical systems are often subdivided into separately owned subsystems. This *multi-owner* structure imposes physical, economic, market, and political constraints on the data transfer. These divisions make systems vulnerable to potential coordinated attacks. Defending against such attacks requires the infrastructures to be more automated and self-healing. Motivated by the challenge of a more efficient, secure and robust power grid, which is less vulnerable to blackouts due to cascaded events, this paper discusses some of the fundamental problems in designing future cyber-physical systems.**

***Index Terms*—Cyber-Physical Systems; Smart Grid; Automated Control; Multi-Owner Infrastructures; Secure Communication**

I. Introduction

Automated control of large-scale physical systems is a challenging problem faced by scientists and engineers in a wide variety of applications including: power grids, transportation networks, and telecommunication networks. The problem requires (i) data collection, (ii) secure data transfer to processing centers, (iii) data processing, and (iv) timely decision making and control actions. These tasks are complicated by the vast amount of data, the distributed sources of the data and the need for efficient data communication. The large physical systems are often subdivided into separately owned subsystems which impose physical, economic, market, and political constraints on data transfer. Further, most large-scale physical systems have multiple owners, and these series of challenges have to take place over a set of domains imposing market constraints. These challenges are emphasized for large-scale *infrastructure* systems where seamless system operation is crucial. In addition, potential coordinated attacks require the infrastructures to be more automated and self-healing. [1] Though examples of such large-scale multi-owner infrastructure systems are many, we focus on the power grid in this paper.

We propose an "Open Cyber-Architecture" (OCA) that enables automated control of multi-owner large-scale infrastructure systems through smart networked substructures. Our proposed architecture promotes information sharing among system owners through a secure information communication and processing paradigm which assures only minimal information sharing. To overcome market inefficiencies, such open sharing of technical information partially takes place in some existing large-scale infrastructures such as the Internet. Our contribution is using optimum information sharing among smart substructures which will filter proprietary information belonging to other owners. We also propose to investigate real-time visualization techniques that will allow human operators to efficiently intervene when necessary or if the owner desires to implement a new policy.

The OCA is centered around the following distinctive features: (a) Highly-dynamic communication protocols, which allow for an adaptive monitoring system that is responsive to changes in the physical environment. (b) Distributed AI algorithms, that provide early autonomous detection of possible catastrophic events, such as cascading of failures in the physical infrastructure, and an autonomous response to such situations. (c) Study of the effects of real but often ignored parameters, such as market constraints, on the autonomous operation of large-scale cyber-infrastructures. (d) Blind communication protocols for cyber-physical systems of competing entities, which do not disclose information to human participant of the financial markets. (e) Decentralized control under market constraints. (f) Importance-based visualization tools that empower human operators of large-scale infrastructures.

Our inspiration for OCA stems from the *power grid* which is a crucial infrastructure that has all the characteristics of the multi-owner large-scale physical systems. It has become clear that the power grid needs decentralization of the Supervisory Control and Data Acquisition System (SCADA) systems so as to have more efficient, secure and robust information exchange. The existing cyber-architecture in the power grid provides limited information exchange among domain owners due to energy market constraints and trust boundaries. This "closed" cyber-architecture makes it difficult to detect potential problems and can lead to catastrophic failures [2] [3] [4] [5]. The OCA focuses on a better grid performance with increased information exchange while respecting the wholesale

energy market constraints, by keeping the actual information shared to a minimum.

Further, the OCA aims to minimize cascading events by introducing decentralized monitoring and control, increased information exchange by new communication structures and replacing the human operators with decentralized automated agents for decision making. New security schemes are considered to enhance the safety of the data communication and network against cyber attacks. A new visualization tool for large scale networks is also needed to provide the user the flexibility for "importance-based" visualization and simulation.

The paper is organized as follows: In the next section, we provide background on the electrical energy markets and lay out the motivating reasons for an open-cyber architecture. Section III describes the major components of the proposed OCA. Then Sections IV and V discuss major research challenges and possible solutions for OCA under open or market constrained information exchange scenarios, respectively. We, then, summarize our work.

II. Background: Making the Case for OCA

The electric power industry in the US was initially designed in the form of "vertically integrated" local systems where the generation, transmission and distribution were owned by one entity. Gradually the demand for electricity of "higher quality" increased and the local systems were interconnected to provide *uninterrupted power, stable voltage* and *stable frequency*. However, the failure of investment in the network to keep up with continued increase in demand resulted in network congestion and vulnerability.

In response, the competitive market system was introduced where the electrical and financial energy markets are governed by independent system operators (ISOs). ISOs are non-profit organizations that comply with the Federal Energy Regulatory Commission (FERC) regulations but are responsible to their shareholders and market participants. The market participants are the power generation owners, transmission line owners, facility owners and financial entities. In some regions there are no competitive markets and the power system operations with bilateral transactions are coordinated by Regional Transmission Organizations (RTOs) or pools. The complexity of the competitive market system arises from the enormous financial interests of the market participants.

As shown in Figure 1 each region is governed by one ISO equipped with a Supervisory Control and Data Acquisition System (SCADA) that collects information (network topology) and data (measurements) from the network and provides it to the Energy Management Systems (EMS) system. The measurements are: magnitude of node voltage, active and reactive power/current flows along a transmission line which are collected in a number of substations. Data is then transmitted via wireless Remote Terminal Units (RTUs) to the central SCADA system in the system operator control room.

Energy Management System (EMS) is used to analyze and monitor the network through the following functions:

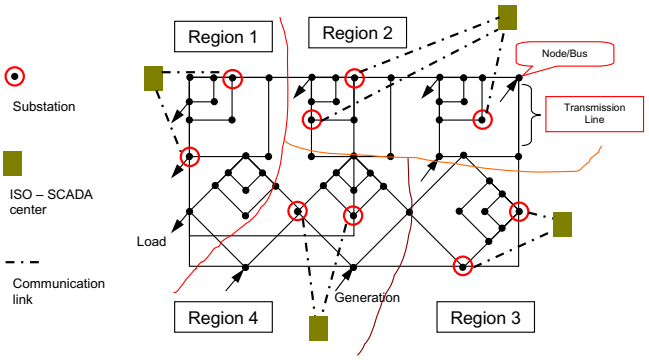


Fig. 1. Current structure with communication links.

- State estimation - to determine the power system state (phasor voltages of the nodes) subject to transmission line thermal limits and bus voltage upper and lower limits as constraints [6] [7],
- Contingency Analysis - to determine the power system state (possible voltage or flow violations) of the network for a preselected set of contingencies [8] [9] [10],
- Security Constrained Unit Commitment - to commit the plants for next day's generation respecting the costs and contingency analysis results [11],
- Security Constrained Optimal Power Flow - to determine the cost of energy subject to cost of generation, transmission line thermal limits, bus voltage upper and lower limits as well as to contingency analysis results [12] [13] [14].

Each ISO monitors and controls its own region and is only provided with the power flow on the "tie" lines connecting it to other regions. Information exchange is necessary for modeling, simulation and decision making within each region. This *limited information exchange* and centralized control with one SCADA system for each system operator makes the system more vulnerable to physical and cyber attacks as well as cascading events. Even though the power system infrastructure is well equipped with automated protective devices to safeguard expensive equipment (generators, transformers, transmission lines and etc.), system operators make the final decision for operating and controlling the system. The extensive human decision making also introduces another degree of complexity.

The blackout in August 2003, which was initiated in Midwest and later affected more than 25 million people in the Northeast, was a direct result of operator error and insufficient information exchange between Midwest ISO (MISO) and Pennsylvania-Jersey-Maryland Interconnection (PJM) [2]. New York ISO, which suffered the blackout, reported that "The NYISO had received no notifications or advisories from other control areas and thus, had no awareness of the precursors to the blackout." [3] [4] As emphasized in North American Reliability Council's report in 2004 [5], the primary weaknesses in need of attention were:

- Reliability Tools: Faster and more accurate topology processors, power system state estimators and real-time contingency analysis tools.

- Visualization Tools: Fast and efficient visualization mechanisms which provide the system status and failures of key lines, generators, or equipment, as well as a high-level voltage profile of the network.
- Communications within the ISO and with its neighboring control areas and reliability coordinators.

The limited information exchange among the operators resembles the traffic signal system of two adjacent cities with interacting traffic flows but limited or no communication between traffic managers. This can result in traffic jams that could be avoided by efficient and optimum coordination between two systems.

The constraints introduced by the market system are obscured by *the financial gains, lucrative auctions* in markets and *opaqueness* of the operation and information exchange related to power systems. This paper addresses the following challenges and proposes decentralized, automated and fast solutions:

- Centralized control within each region for steady-state operation.
- Human decision making.
- Insufficient information exchange between the ISO regions.
- Unavailability of a real-time snapshot of the interconnected power system as a whole.

III. Open Cyber-Architecture (OCA)

The main goal of our proposed Open Cyber-Architecture (OCA) is to enhance reliability and efficiency of large-scale multi-owner physical infrastructure systems. The existing systems typically use a centralized cyber-architecture and strictly hide proprietary information from some of the other owners. Though a "closed" approach (as in Figure 3-a) hiding proprietary information makes sense in terms of business goals, the technical viability of the overall system depends on safe and sufficient sharing of basic technical information in a relatively "open" manner (as in Figure 2). Information sharing among owners is critical to attain the needed robustness for infrastructure systems. The key proposition of OCA is to provide the means to increase information sharing through more regulated means and essentially make it part of the physical system itself even to the extent that the owners may not be able to avoid sharing of some of the market related information.

The basic idea of sharing required information has successfully been implemented in large-scale systems. For instance, the Internet requires its participants to provide some basic connectivity information to be part of the larger connected network. This implicit reinforcement of information sharing is mainly driven by the "fate sharing" that naturally exists in the overall system. Participants become willing to share information (and potentially other resources) in order to make "the whole ship float". OCA aims to extend this paradigm to other large-scale infrastructure systems.

We abstract components of OCA as follows:

- **Integrated Secure Communication** to provide the means to share information among subsystems (or components) of the infrastructure.
- **Self-Healing via Automated Control** that can use shared information while safeguarding market constraints and can handle large amounts of information in crises at speeds beyond human capabilities.
- **Distributed Planning via Smart Subsystems** to provide individual components with the planning and learning capability required for a robust infrastructure than can respond to unexpected events.
- **Effective Human Interface,** including visualization tools, that will allow human operators to effectively utilize the available data to implement business policies or deal with emergencies.

Figure 3-b summarizes the components of OCA by comparing them to the existing Closed Cyber-Architecture of physical infrastructure systems.

IV. OCA: Free Information Exchange

A. Importance-Based Network Protocols

In the OCA, the smart substations of the power grid will be interconnected through a communication network "integrated" with the power system infrastructure. Unlike the existing communication architecture, the OCA's smart substations will be part of a self-operating communication network. The major goals of this integrated communication network include (i) reliable delivery of state estimation data to other smart substations, (ii) in-network aggregation of intra-ISO data before sending them to other ISOs, and (iii) timely and efficient delivery of important event data to the interested ISOs or smart substations.

Reliable Delivery of Critical Infrastructure State Information: The Internet has served as a communication medium for power operators [15]. Similarly, in a report presented to congress on preventing blackouts, the Department of Energy has proposed to build a real-time transmission monitoring system that utilizes the Internet [16]. However, critical infrastructures have specific service requirements, such as timely delivery and minimum bandwidth, that are not guaranteed by the Internet. Since the Internet's core protocols provide best effort delivery, it cannot provide an acceptable infrastructure for communication between smart substations. Thus, a new network model that will sustain communication requirements of critical infrastructures like the power grid is needed.

In addition to general service requirements, cyber security is a major requirement for the communication backbone of the power grid. For instance, SCADA systems have been the target of attacks generated through the Internet [17]. Having a dedicated network for critical infrastructures will significantly limit the network's vulnerability. Moreover, the Internet is not inherently secure as its initial design assumed trusted users [18]. Hence, a new suite of communication protocols that will include security from the outset is needed.

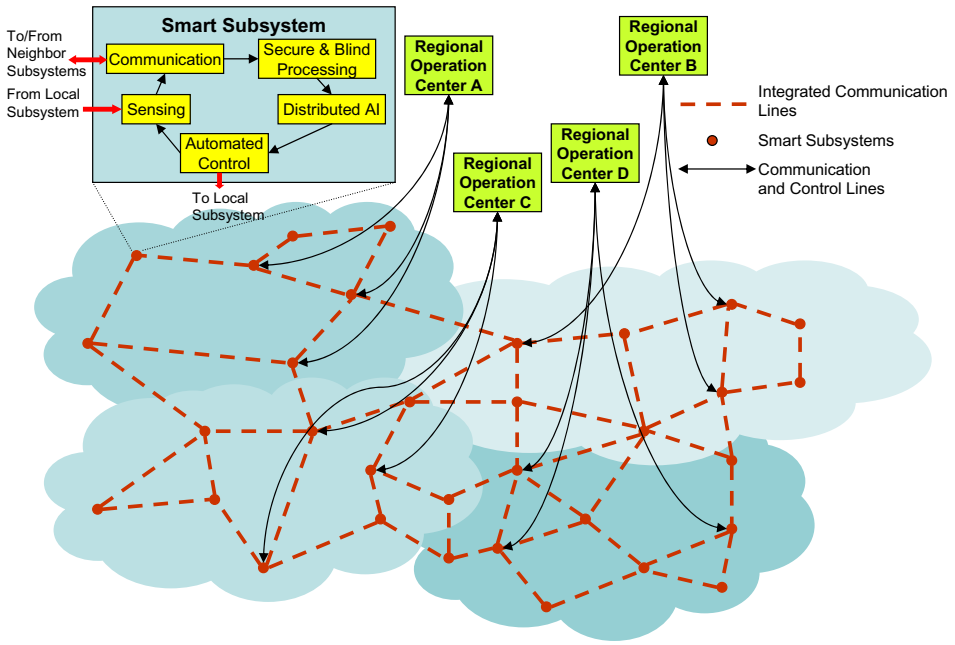
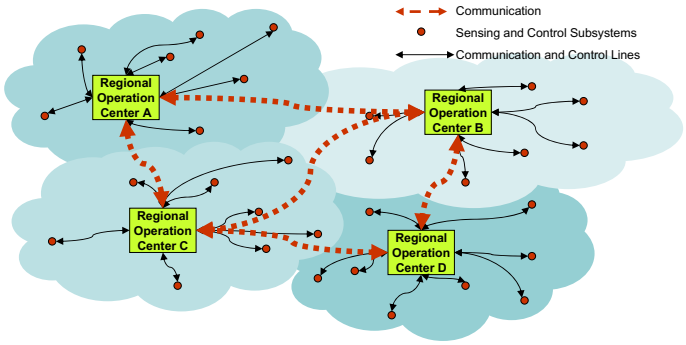


Fig. 2. Open Cyber-Architecture: Information sharing is integrated into the physical system and takes place at operational time-scales. Such fine-granularity and open communications enable distributed decision-making mechanisms and self-healing automated control of the physical system.



(a)

Open Cyber-Architecture	Closed Cyber-Architecture
distributed decision-making at smart subsystems	centralized decision-making at operation centers
integrated, device-level, open communications	disparate, domain-level, proprietary communications
increased automated control	manual, human-driven control
reactive human involvement only in emergencies	proactive human involvement with online operator

(b)

Fig. 3. Closed Cyber-Architecture in the existing physical infrastructure systems and comparison with the OCA. (a) Closed Cyber-Architecture: Information sharing takes place at large time-scales and control is limited within a domain. Decision making happens at centralized locations. (b) Comparison of major features of Open Cyber-Architecture against the existing Closed Cyber-Architecture physical systems.

In-Network Aggregation and Filtering of Intra-ISO State: Data aggregation to minimize transmission power consumption has been extensively analyzed in sensor networks [19], due to limited sensor power. However, sensor energy is not a major constraint in power systems. Hence, in OCA, alternative data aggregation algorithms that will minimize traffic and reduce computation at smart substations can be developed. Such data processing functions can be implemented at the substations located on ISO boundaries. The purpose will be to filter some of the critical proprietary information from other ISOs and aggregate large amount of intra-ISO state information before sending to other ISO domains.

Importance-Based Routing and Data Dissemination: Due to the large size of the power grid, disseminating all the state data sensed at substations is impractical, and routing based on the importance of the data is usually necessary. Previous research studied priority/value-based forwarding [20] (with support from intermediate router queues), but did not consider a routing scheme explicitly accounting for importance of data on an end-to-end basis (i.e., without requiring router support).

For OCA, we consider a two-stage data dissemination architecture for realizing importance-based routing: (i) *proactive flooding* of the minimum state data required (e.g., voltage and current levels of major power transmission lines) to detect risk of an important event (e.g., failure of a power transmission line), and (ii) *reactive on-demand transfer* of detailed state data following detection of a risk of a major event. Though the amount of data to transfer will be small in the proactive stage, the reactive stage must cope with almost simultaneous transfer of huge amounts of data. This is standard practice for the power grid where an event will trigger many operators and smart substations to ask for detailed information about the grid topology in its vicinity. This "flash crowd" phenomenon exists in many networked systems (e.g., peer-to-peer) [21]

as the demand profile is quite conceivably heavy-tailed. The complexity of the problem is higher in the power grid since the set of substations/operators interested will be different for each "event". Thus, one promising approach is to support this reactive transfer stage with multicast.

B. Mitigating Cascading Events

Today's infrastructure can accommodate a single point of failure such as a failed transmission line but multiple failures can lead to cascading events, which may cause the collapse of the entire network. Current preventive schemes depend on human expertise to predict the behavior of the grid under different failure situation. The envisioned system aims to assist the human operator by considering a larger set of contingencies and automatically suggesting preventive actions.

Formalization: The power grid involves both discrete and continuous processes and a formalization as a stochastic hybrid system (SHC) could be used. A SHC has:

- A continuous state $x \in \mathcal{X}$, involving the voltage profile and the power flow on the grid.
- A discrete state $q \in \mathcal{Q} = \{1, 2, ..., N\}$, such as grid failures or modes of operation.
- The undesirable subset $\mathcal{X}_f \subset \mathcal{X} \times \mathcal{Q}$ (e.g., states where the grid has failed).
- Controls $u_d \in \mathcal{U}_d$ (e.g., level of load generation) and plans: $p_d(T) = \{u_d(dt_1), ..., u_d(dt_n)\}$ ($T = \sum_i dt_i$).
- Stochastic inputs $u_s \in \mathcal{U}_s$ (e.g., renewable energy generation) [$p_s(T) = \{u_s(dt_1), ..., u_s(dt_n)\}$].

The dynamics of a SRC are then represented by the continuous dynamics: $\dot{x} = f(x, u_d, u_s, q)$, the jump set between nodes $x \notin J(x, u_d, u_s, q)$ and the discrete transition map $(x, q)^+ = v(x, u_d, u_s, q), x \in J(x, u_d, u_s, q)$. When $p_d(T)$ and $p_s(T)$ are applied to state (x, q) for time T, then the system follows a path: $\pi(t)$ $((x, q), p_d(T), p_s(T))$. The plan $p_d(T)$ is selected by a planning algorithm, while $p_s(T)$ is stochastic and the resulting path has an associated probability. The set of paths of duration T, applied at location (x, q), which intersect $\mathcal{X}_f$, are: $\pi_{\mathcal{X}_f}((x, q), T) = \{ \forall\ p_d(T),\ p_s(T) \mid \pi(t)((x, q), p_d(T), p_s(T)) \cup \mathcal{X}_f \neq 0 \}$. Then, the following problem arises: *For horizon T, current state (x_c, q_c) and current plan $p_d(T)$, what is the cumulative probability of paths in the set $\pi_{\mathcal{X}_f}((x_c, q_c), T)$? (verification)* If paths $\pi_{\mathcal{X}_f}((x_c, q_c), T)$ do exist and have high probability, then the system has a high probability of reaching an undesirable state. This action selection process corresponds to the problem: *Which $p_d(T)$ minimizes the cumulative probability of undesirable paths in $\pi_{\mathcal{X}_f}((x_c, q_c), T)$? (planning).*

Detecting and predicting cascading events: Tentatively assume the current state (x_c, q_c) is always available to a centralized operation center where verification must be solved for a horizon T. Then *sample* potential paths initiated at (x_c, q_c) for a given plan $p_d(T)$ and different stochastic inputs $p_s(T)$. Assuming knowledge of the probability of a stochastic input $u_s(dt)$ given a state: $P(u_s(dt)|(x(t), q(t))$, where $t \in [0, T)$ and $dt \leq T - t$, we can apply the following sampling-based approach:

- Sample $(x(t), q(t))$ already connected to (x_c, q_c) via a path according to: $P((x(t), q(t))|(x_c, q_c))$.
- Compute $P(u_s(dt)|(x(t), q(t)))$ and sample a stochastic input $u_s(dt)$.
- Obtain the corresponding control $u_d(dt)$ from the current plan $p_d(T)$.
- Propagate the corresponding local path $\pi((x(t), q(t)), u_d(dt), u_s(dt))$.
- For all resulting states $(x(t'), q(t'))$ along the local path, compute $P((x(t'), q(t'))|(x_c, q_c)$.
- Repeat until no more time is available, i.e. $t = T$.

The objective is to estimate $P_{\mathcal{X}_f}$: the probability the sampled paths $\pi_{\mathcal{X}_f}((x, q), T)$ intersect $\mathcal{X}_f$. When $P_{\mathcal{X}_f}$ is high, then the system is in danger and an action is required. To compute the appropriate plan, a similar sampling-based approach can be employed. For each sampled state $(x(t), q(t))$, it is possible to sample among the set of valid controls $u_d(dt)$. The sampling distribution will affect the performance of the search procedure. The above procedures raise the following issues:

- *Computational challenges:* The search must be efficient.
- *Time horizon:* A limited horizon may force the system to a state $(x(T), q(T)) \notin \mathcal{X}_f$ that inevitably leads to $\mathcal{X}_f$.
- *Probabilistic models:* Only approximations of the probabilities (e.g., $P(p_s(T)|(x_c, q_c))$) are available.
- *Comparison against current mode of operation:* Can the algorithm identify a cascading event before a human operator can and does it select different actions?

Decentralized, Message-Passing Operation: State variables and controls can be decomposed into local terms for each substation. The substations must coordinate to select a joint plan $p_d(T) = \{p_d^1(T), \ldots, p_d^n(t)\}$. To achieve this, it is possible to incorporate message-passing tools for distributed constraint satisfaction. An objective function W must be defined that is decomposable into local utility functions W^i for each substation: $W = \sum_i W^i$. To mitigate cascading events, W^i are maximized when the i-th substation is operating effectively, which will result in efficient operation of the overall system. A local W^i function coordinates substation actions since it depends on the actions of the i-th substation and its neighbors. Such dependencies can be represented using a coordination graph $G(V, E)$, where a node corresponds to a substation and an edge represents dependencies between substations. Then the objective function can be rewritten as a sum of unary and pairwise utility terms: $W = \sum_{i \in V} W(u_d^i) + \sum_{(i,j) \in E} W(u_d^i, u_d^j)$, which must be optimized in a distributed manner.

V. OCA: Market Constrained Information Exchange

A. Securing the Inter-ISO Communication Infrastructure

The power communication infrastructure must be secured against cyber attacks and malfunctioning components. Terrorist organizations are aiming at infiltrating control systems of critical infrastructures [22]. A cyber attack on the power

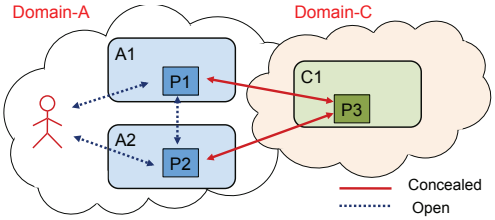


Fig. 4. Securing inter-domain messages

communication infrastructure may not only damage the power grid itself but other critical infrastructures as well due to their dependence on the energy. Moreover, the smart substations will have greater dependence on the communication infrastructure. A vulnerability in the smart grid will have a greater impact on the power system than the current substations. It is important to include cyber security as a core element for all system components including measurement devices.

We propose a *blind communication* mechanism to exchange sensitive data between processes at different systems and improve information sharing between competing entities [23]. The goal in blind processing is to establish a secure communication channel which is concealed from even system administrators. The sensitive data is transmitted through the secured channel and used in computations running in an isolated environment while the outcome is rendered only to a dedicated user or a process. Shielding information prevents gaining access to the sensitive data while providing a complete picture of the whole system and remedies the effects of energy market constraints and trust boundaries over the operation of the power grid infrastructure.

For blind processing, we need a mechanism to restrict the behavior of each remote system and prevent data leakage. *Trusted computing* [24] has a potential to provide a basis for the blind processing service. Trusted functionality of a system is furnished by a *Trusted Platform Module* (TPM) where the TPM serves as the *root of trust* that an operating system and higher level applications can build upon. The TPM is a secure cryptoprocessor mounted on the motherboard of a system to provide assurance of conformed operation of the host system to both local and networked applications. An important aspect of the TMP is to measure the integrity of a system without compromising results to a potentially malicious host system. TPM essentially provides cryptographic primitives, integrity measurement to ascertain the system state, sealing of sensitive data to a certain system state, and globally unique identification for its host system. Cryptographic keys generated by TPM can be utilized to exchange information between trusted processes that shield its data. Using a secure communication protocol, a remote system can request measurement results to detect modifications in the system. In particular, remote platform attestation mechanism gives assurance that the system is at a conformed state to a remote entity.

Using blind communication security services, remote parties will be able to exchange sensitive data through isolated processes whose execution environment and data is shielded from the rest of the system. We present a conceptual model of the blind communication between two processes where we consider a multi-owner networked system to be composed of *ally* and *competitor* processes in Figure 4. Processes generate or collect data and (partially) share the data with other processes including the competitors. The data is openly, but securely, transferred to the allies in the same domain. However, when data is being transferred to a system in a competitor's domain, the data will be concealed at its destination. For instance, the operator in Figure 4 can view messages from A1 and A2 but has no access to messages from C1.

In *blind processing*, the TPM chips will be utilized to encrypt messages transmitted to both ally and competitor systems. To provide a secure execution environment to trusted processes, the remote system will prevent external processes from accessing protected memory locations using a security kernel [25]. Using a security kernel ensures that trusted blind processing is executed in a sandbox safe from tampering. Moreover, stored data will be encrypted using storage keys shielded in the TPM. The storage root key will be used to develop a key chain that will be used to encrypt data and bind it to a certain trusted system state. The state measurements will help verify any alteration in the system state and prevent the TPM from decrypting any sealed data when there is a modification to the underlying system or trusted processed.

When communicating with a remote process, a system must identify the process to prevent unauthorized access. A credential verification mechanism is required to authenticate systems from the same domain and other domains. TPM authenticates with a Privacy Certificate Authority (CA) using its Endorsement Key (EK) and other credentials to obtain a digital certificate for the generated Attestation Identity Keys (AIK), an alias identity. The AIKs are then used to establish the identity and the authenticity of a remote party. In our case, each domain needs its own CA independent of other domains since EKs mus be private to each domain. EKs are permanent and cannot be revoked in case it is deciphered. Having a separate CA for each domain requires a mechanism to authenticate processes from other domains. This can be achieved by ensuring identities in a hierarchical manner.

We can utilize secure root processes of the TPM to develop authenticators that will ensure the integrity of processes using the CRTM [26]. Integrity evaluation involves verifying the source, its integrity, and freshness of the measurements and requires the knowledge of fingerprints (i.e., SHA-1 hashes) of the code involved in the blind processing. To ensure the integrity of a system, a remote challenger will first request measurements of the communicating process. The challenged system will obtain relevant PCR values signed with the private AIK and gather corresponding SML entries. The signed PCR and SML values will be sent to the challenger along with credentials for the AIK. The challenger will then inspect the supplied credentials, analyze the SML to conform the system state by examining the sequence of events, and verify system integrity by comparing PCR values with stored fingerprints.

The fundamental problem that motivates the blind com-

munication is to alleviate market constraints on information sharing between operators in the power grid. As emphasized in the 2004 North American Reliability Council's report, one of the primary weaknesses in need of the attention is "communications within the ISO and with its neighboring control areas and reliability coordinators" [3]. With sensing information from all system components, ISOs can independently monitor the health of the power grid. Secured computing systems can gather information from other ISO's sensing devices but hide the information from human operators. Shielding information even from the system administrators protects commercially sensitive data while allowing the EMS to obtain a better picture of the power grid and more accurately detect and mitigate disturbances. The increased information sharing will also enhance the adaptability of the power grid with the proliferation of distributed renewable energy generation that provides intermittent energy.

B. Distributed Control under Market Rules

Decentralized control is a well known problem in the control literature that has received considerable attention over the last few decades [27],[28]. Networked control is a more recent area of interest which considers the effect of significant sensor and actuator delays in the control network. More recently, researchers have considered decentralized networked control and its implications. Typically, a set of identical systems is considered with quantitative constraints on their interaction [29],[30]. In many practical situations, the subsystems are significant different and the assumption of identical subsystems is invalid. In addition, the constraints on interaction are qualitative rather than quantitative and traditional methodologies are no longer applicable.

Consider the nonlinear network dynamics:

$$\begin{aligned} &\dot{x} = A_i x_i + B_i u_i + f_i(\bar{x_i}, u), \\ &y_i = C_i x_i + g_i(\bar{x_i}, u), \qquad i = 1, ..., N \end{aligned} \tag{1}$$

where x_i, u_i and y_i are the state, control and output, and (A_i, B_i, C_i) are the (state, input, output) matrices of the ith subsystem. The interaction of the state with of the ith subsystem with the remainder of the system is represented by the function $f_i(\bar{x_i}, u)$ where the vector $\bar{x_i}$ denotes the state vector with the state of the ith subsystem removed. The state and control of the overall system are related to those of the subsystems by

$$x = col\{x_1, ..., x_N\}, \qquad u = col\{u_1, ..., u_N\} \tag{2}$$

The interaction between subsystems is subject to market and political constraints that cannot be described using traditional mathematical techniques. These constraints can be represented as a set of Takagi-Sugeno (TS) fuzzy rules of the form [31] [32]

$$IF(Premise)THEN(formula) \tag{3}$$

where formula is a static or dynamic mathematical model. For example, different models can be used in the analysis of large power networks based on the interests of the modeler and the information available. This qualitative form of information is often ignored when dealing with engineering systems because of the engineering culture of over-reliance on quantitative methods. Note that the above constraints differ from those of fuzzy linear programming [33].

A problem of fundamental importance is the stability of the large scale system in the presence of fuzzy constraints. For Mamdani systems the approach of [34] provides an excellent methodology based on Lyapunov stability theory. For TS systems the stability problem was reviewed by Sugeno in [35] and most of the results available require a common Lyapunov function in all regions of operation. This severe restriction was removed using a Lyapunov approach by Sonbol and Fadali for the discrete time [36] and continuous time [37] cases. A combination of the approaches of [34] and [37] is needed to analyze the stability of large scale systems with fuzzy rule constraints.

The results of [34] also offer an attractive approach to fuzzy system optimization that can be extended to large-scale systems with fuzzy rule constraints and used in the analysis of the smart grid. The approach uses the hyperbolic model

$$\begin{aligned} &\dot{x} = Ax + Bu, \qquad y = [y_1 ... y_n]^T, \\ &y_i = \tanh(k_i x_i), \qquad i = 1, ..., n \end{aligned} \tag{4}$$

with the optimality criterion

$$min \int_0^\infty \{y^T Q y + u^T R u\} dt \tag{5}$$

for the hyperbolic system. The optimal solution is in the form $u = Hy$, where H is an m by n constant matrix. However, Margaliot et al. [34] do not consider the effect of fuzzy rule constraints on their design. Neither do they consider the case of a decentralized large-scale system. OCA requires their approach to be extended for accommodating fuzzy rule constraints including both Mamdani and TS types. Decentralized designs for large-scale scenarios and the impact of their interaction on the fuzzy designs must be investigated.

VI. OCA: Hierarchical, Multi-Resolution, Importance-based Visualization of Power Grid

A sensor network is essential to provide the information needed to monitor any large-scale system. Measurements obtained throughout the network will always include uncertainties that must be accounted for with redundant measurements. Practical and economic considerations limit the level of sensor redundancy and some redundant information may not be fully exploited. Visualization tools can provide the best possible exploitation of all available data because they facilitate their utilization by human operators throughout the system.

With power systems, the need for complex massive representations of concepts and results [38] is great. For our OCA, visualization of the data is crucial since it is this understanding which we seek in order to improve power grid operations. Visualization tools for the power grid must be capable of zooming in/out through a hierarchical and multi-resolution plane. Further, importance-based visualization modules are

needed as the constraints of the network must be involved in the visualization for the visualization tool to act as an efficient warning and decision aid during an emergency. The key technical tool for such visualization will be graph algorithms, such as Steiner Minimal Trees [39] and minimum crossing number techniques [40], to represent power grids in a two-dimensional plane.

VII. Summary

In this paper, we proposed a new cyber-architecture, the OCA, for large-scale physical infrastructure systems with a focus on the power grid. By using smart networked substructures, the OCA focuses on handling market and operation constraints arising due to the multi-owner nature of such physical infrastructures. We laid out the motivating reasons for the OCA within the context of the electrical power grid. We outlined major components of the OCA as (a) a secure communication capability integrated with the physical components, (b) an increased automated control for a self-healing, (c) a distributed planning framework to mitigate cascading events, and (d) an effective human interface for operators. We discussed the research challenges in achieving these OCA components under "open" or "closed" scenarios, where information sharing among domains is allowed or market-constrained.

References

[1] J. Miller, "Research on the characteristics of a modern grid: Operates resiliently against attack and natural disaster," *Energy Pulse*, vol. 4, no. 3, February 2009.

[2] U.-C. P. S. O. T. Force, "Final report on the august 14,2003, blackout in the united states and canada: Causes and recommendations," U.S. Department of Energy, Washington, D.C., Tech. Rep., April 2004.

[3] N. Y. I. S. Operator, "Interim report on august 14, 2003 blackout," NYISO, Albany, NY, Tech. Rep., January 2004.

[4] ——, "Blackout august 14, 2003 final report," NYISO, Albany, NY, Tech. Rep., February 2005.

[5] N. A. E. R. Council, "Technical analysis of the august 14, 2003, blackout:what happened, why and what did we learn?" NERC, Princeton, NJ, Tech. Rep., July 2004.

[6] F. C. Schweppe and J. Wildes, "Power system static-state estimation-part 1: Exact model," *IEEE Trans. On Power Appratus and Systems*, p. 120, January 1970.

[7] O. Alsac, N. Vempati, B. Stott, and A. Monticelli, "Generalized state estimation," *IEEE Trans. on Power Sys.*, vol. 13, no. 3, p. 1069, August 1998.

[8] Hanson and Bose, "Input-output processing of online contingency analysis," *IEEE-PICA*, p. 58, 1979.

[9] A. Alves and Monticelli, "Critical evaluation of direct and iterative methods for solving ax=b systems in power flow calculations and contingency analysis," *IEEE Trans. On Power Sys.*, vol. 14, no. 2, p. 702, May 1999.

[10] R. Santos, G. Exposito, and M. Ramos, "Distributed contingency analysis: practical issues," *IEEE Trans. On Power Sys.*, vol. 14, no. 4, p. 1349, November 1999.

[11] J. D. Guy, "Secutity constrained unit commitment," *IEEE Trans. On Power Appratus and Systems*, vol. PAS-90, no. 3, p. 1385, May 1971.

[12] O. Alsac and B. Stott, "Optimal load flow with steady state security," *IEEE Trans. On Power Appratus and Systems*, vol. PAS-93, p. 745, May/June 1974.

[13] J. Carpentier, "Optimal power flows," *International Journal of Electrical Power and Energy Systems*, vol. 1, p. 3, April 1979.

[14] R. Baldick, B. H. Kim, C. Chase, and Y. Luo, "A fast distributed implementation of optimal power flow," *IEEE Trans. On Power Sys.*, vol. 14, no. 3, p. 858, August 1999.

[15] "Cryptographic protection of scada communications," American Gas Association, Mar 2006.

[16] "Steps to establish a real-time transmission monitoring system for transmission owners and operators within the eastern and western interconnections," U.S. Department of Energy & Federal Energy Regulatory Commission, Feb 2006. [Online]. Available: http://www.oe.netl.doe.gov/docs/prepare/21stepsbooklet.pdf

[17] A. Greenberg, "Hackers cut cities' power," Forbes, Jan 2008.

[18] C. E. Landwehr, David, and M. Goldschlag, "Security issues in networks with internet access," in *Proceedings of the IEEE, Volume 85, Issue 12*, 1997, pp. 2034–2051.

[19] R. Rajagopalan and P. K. Varshney, "Data aggregation techniques in sensor networks: A survey," *Communications Surveys & Tutorials, IEEE*, vol. 8, pp. 48–63, 2006.

[20] M. E. Sisselman and W. Whitt, "Value-based routing and preference-based routing in customer contact centers," *Production and Operations Management*, vol. 16, no. 3, pp. 277–291, 2007.

[21] T. Stading, P. Maniatis, and M. Baker, "Peer-to-peer caching schemes to address flash crowds," in *Proceedings of the Workshop on Peer-to-Peer Systems (IPTPS)*, 2002.

[22] J. Hamre, "Cyberwar! interview with john hamre," PBS Frontline, Feb 2003. [Online]. Available: http://www.pbs.org/wgbh/pages/frontline/shows/cyberwar/interviews/hamre.html

[23] M. H. Gunes and C. Y. Evrenosoglu, "Blind processing: Securing data against system administrators," in *IFIP/IEEE International Workshop on Management of Smart Grids*, Apr 2010.

[24] "Trusted computing group," (http://www.trustedcomputinggroup.org). [Online]. Available: http://www.trustedcomputinggroup.org

[25] B. Pfitzmann, J. Riordan, C. Stble, M. Waidner, and A. Weber, "The PERSEUS system architecture," IBM Research Division, Tech. Rep., 2001. [Online]. Available: http://www.perseus-os.org/

[26] M. Alam, X. Zhang, M. Nauman, T. Ali, and J.-P. Seifert, "Model-based behavioral attestation," in *SACMAT '08: Proceedings of the 13th ACM symposium on Access control models and technologies*. New York, NY, USA: ACM, 2008, pp. 175–184.

[27] M. Jamshidi, *Large Scale Systems: Modeling Control and Fuzzy Logic*. Upper Saddle River, NJ: Prentice-Hall, 1997.

[28] D. D. Siljak, *Decentralized Control of Complex Systems*. Boston: Academic Press, 1991.

[29] B.Bamieh and P. Voulgaris, "A convex characterization of distributed control problems in spatially invariant systems with communication constraints," *Syst. Control Lett.*, vol. 54, pp. 575–583, 2005.

[30] F. Borelli and T. Keviczky, "Distribued lqr design for identical dynamically decoupled systems," *IEEE Trans. Automat. Contr.*, vol. 53, no. 8, pp. 1901–1912, 2008.

[31] R. F. C. Carlsson and S. Giove, "Optimization under fuzzy linguistic rule constraints." Budapest, Hungary: SIC'99, May 1999.

[32] H.-f. L. X. Luo; J. H.-m. Lee and N. R. Jennings, "Prioritised fuzzy constraint satisfaction problems: axioms, instantiation and validation," *Fuzzy Sets and Systems*, vol. 136, pp. 151–188, 2003.

[33] X. L. Wang, *A Course in Fuzzy Systems and Control*. Upper Saddle River, NJ: Prentice-Hall, 1997.

[34] M. Margaliot and G. Langholtz, "New approaches to fuzzy modeling and control: Design and analysis." Singapore: World Scientific, 2000.

[35] M. Sugeno, "Stability of fuzzy systems expressed by rules with singleton consequents," *IEEE Trans. Fuzzy Systems*, vol. 7, no. 2, pp. 201–224, April 1999.

[36] A. Sonbol and M. S. Fadali, "Stability analysis of discrete tsk types ii/iii fuzzy systems," *IEEE Trans. Fuzzy Systems*, vol. 14, no. 5, pp. 151–188, October 2006.

[37] ——, "Tsk fuzzy systems types ii and iii stability analysis: Continuous case," *IEEE Trans. Systems Man and Cybernetics*, vol. 36, no. 1, pp. 151–188, 2006.

[38] E. P. R. Institute and U. D. of Defense, "Complex interactive networks/systems initiative: Final summary report: Overview & summary report for joint electric power research institute and u.s. dod university research initiative," Electric Power Research Institute and U.S. Department of Defense, EPRI, Palo Alto, CA & U.S. DOD Washington, D.C., Tech. Rep., 2002.

[39] J. F. C. Harris, "Steiner minimal trees: Their computational past, present, and future," *J. Combin. Math. Combin. Comput.*, vol. 30, pp. 195–220, 1999.

[40] J. R. Fredrickson, B. Yuan, and J. F. C. Harris, "A time saving region restriction for calculating the crossing number," *Congr. Numer.*, vol. 168, pp. 145–158, 2004.